Attachment E

FOCUS AREA E: HEALTH ALERT NETWORK/COMMUNICATIONS AND INFORMATION TECHNOLOGY

Focus Area E includes four **Critical Capacities**:

A. Communications Connectivity
B. Emergency Communications
C. Protection of Data and Information Systems
D. Secure Electronic Exchange of Public Health Information

Focus Area E also includes two **Enhanced Capacities**:

E. Support of Emergency Response Management
F. Full Information Technology Support and Services

Each Focus Area includes Critical Capacities, which are the core expertise and infrastructure that should be implemented as soon as possible to enable a public health system to prepare for and respond to bioterrorism, other infectious disease outbreaks, and other public health threats and emergencies. Some of the Critical Capacities include Critical Benchmarks, which recipients are required to complete prior to submission of the work plan (see Notice of Cooperative Agreement Award). Further, some Critical Capacities have associated with them Activities That May be Considered. Though not exhaustive, these lists provide examples of related activities that applicants may propose to develop to augment the relevant Critical Capacity.

For each Critical Capacity, the work plan must provide: (a) a brief description of the existing capacity in your jurisdiction, (b) an assessment of whether this capacity is adequate, and (c) where you judge the capacity inadequate, a proposal for effecting improvements during this budget period--including a timeline to guide implementation, measurable milestones to facilitate accountability, and a proposed budget. This document should not exceed 5 pages.

Each Focus Area also includes Enhanced Capacities, which are the additional expertise and infrastructure--i.e., over and beyond the Critical Capacities--to enable public health systems to have optimal capacities to respond to bioterrorism, other infectious disease outbreaks, and other public health threats and emergencies. Enhanced Capacities should be addressed only after

Critical Capacities have been achieved or are well along in development. Recipients are encouraged to choose among these suggested activities or propose other comparable ones.

For each Enhanced Capacity that the recipient chooses to address now, the work plan must include a brief proposal for effecting the intended enhancements during this budget period--including a timeline to guide implementation, measurable milestones to facilitate accountability, and a proposed budget. This document is not to exceed 5 pages.

RECIPIENT ACTIVITIES:

A. CRITICAL CAPACITY: to ensure effective communications connectivity among public health departments, healthcare organizations, law enforcement organizations, public officials, and others as evidenced by: a) continuous, high speed connectivity to the Internet; b) routine use of e-mail for notification of alerts and other critical communication; and c) a directory of public health participants (including primary clinical personnel), their roles, and contact information covering all jurisdictions.

1. Prepare a timeline for a plan that ensures that 90 percent of the population is covered by the Health Alert Network.
CRITICAL BENCHMARK #11

2. Prepare a timeline for the development of a communications system that provides a 24/7 flow of critical health information among hospital emergency departments, state and local health officials, and law enforcement officials.
(CRITICAL BENCHMARK #12

3. Building on the Critical Benchmark above, assess the existing communication connectivity in your jurisdiction and determine whether this capacity is adequate. **If not, improve this capacity during this budget cycle by:**

a. ensuring that at least 90 percent of your population is covered by state and local health agencies that have these capabilities (see Appendix 6, IT Functions and Specifications);

b. providing for a 24/7 flow of critical health information including alerts (see Appendix 6, IT functions #7-9) and critical event data (see Appendix 6, IT functions #1-3) among hospital emergency departments, state and local public health officials, law enforcement, and other key participants; and

c. ensuring that the directory information (see Appendix 6, IT function #7) is up to date and complete.

4. Activities that may be considered:

a. Inventory existing communication capabilities in relation to existing standards as outlined in the IT Functions and Specifications Appendix.

b. Routinely assess the delivery of e-mail messages to recipients with documentation that the messages have been read.

c. Regularly exchange directory information with key stakeholders and partners**.**

d. Establish and enhance a Web site that contains current and relevant public health information, including health alerts, advisories, and updates. (See Appendix 6, IT functions #8-9.)

B. CRITICAL CAPACITY: to ensure a method of emergency communication for participants in public health emergency response that is fully redundant with e-mail.

1. **Assess the capacity in your jurisdiction for redundant communication devices (two-way radios, cell phones, voice mail boxes, satellite phones, or wireless messaging), the capacity of existing systems at the state and local level to broadcast and/or autodial to automatically distribute alerts and messages to these devices, and the capacity to link to the emergency communication systems of local emergency response partners. If necessary, make improvements during this budget cycle.**

2. Routinely assess the timeliness and completeness of the redundant method of alerting as it exists to reach participants in public health response.

3. Activities that may be considered:

a. Develop broadcast auto-dialing voice messaging capabilities.

b. Provide for technological and staffing redundancy of critical information and communication systems to support these functions. (See Appendix 6,

IT function #9.)

c. Implement a second method of receiving critical alerts such as pagers, cell phones, voice mail boxes, or other devices to allow public health participants to receive alerts in full redundancy with e-mail.

C. CRITICAL CAPACITY: to ensure the ongoing protection of critical data and information systems and capabilities for continuity of operations. (See Appendix 6, IT function #8.)

1. Assess the existing capacity in your jurisdiction regarding **policies and procedures for protecting and granting access to secure systems for the management of secure information, system backups, and systems redundancy. If necessary, develop a proposal for improvements during this budget cycle.**

2. Perform regular independent validation and verification of Internet security, vulnerability assessment, and security and continuity of operations practices, and rapidly implement recommended remedial activities.

3. <u>Activities that may be considered:</u>

a. Establish a firewall for the protection of critical information resources from the Internet.

b. Implement Public Key Encryption (PKI) or equivalent methods of strong authentication for remote access from the Internet.

c. Develop role-based authorization technology and processes to ensure selective authorization to information resources.

d. Institute server- and client-based virus checking software to protect critical systems.

e. Contract with an independent IT security firm to perform ongoing penetration testing and vulnerability analysis.

f. Integrate all remote access to health department IT resources using commercial, off-the-shelf products for a single method of authentication.

g. Implement software systems and/or servers to support Critical Capacities

elsewhere in this guidance. Provide training and support on these systems to improve the ability of public health participants to effectively use them.

D. CRITICAL CAPACITY: to ensure secure electronic exchange of clinical, laboratory, environmental, and other public health information in standard formats between the computer systems of public health partners. Achieve this capacity according to the relevant IT Functions and Specifications.

5. Assess the existing capacity in your jurisdiction to **exchange electronic data in compliance with public health information and data elements exchange standards, vocabularies, and specifications as referenced in the NEDSS initiative. (See Appendix 6, IT functions #1-9.) If necessary, develop a proposal for improvements during this budget cycle.**

2. Ensure that the technical infrastructure exists to exchange a variety of data types, including possible cases, possible contacts, specimen information, environmental sample information, lab results, facilities, and possible threat information. (See Appendix 6, IT functions #1-9).

3. Regularly confirm the successful transmission and receipt of information to and from public health partners.

4. **Activities that may be considered:**

a. Develop firewall capabilities and Web technology and expertise to implement and maintain a ebXML-compliant SOAP service for the secure exchange of information over the Internet.

b. Develop systems and databases to implement the specifications, vocabularies, and standards to exchange like data with public health partners.

c. Implement message parsing technology to allow for the creation and processing of public health information messages.

d. Participate in national stakeholders meetings, data modeling activities, and joint application development sessions to help specify the data types that will be exchanged among public health partners and to understand how to implement them.

E. ENHANCED CAPACITY: to provide or participate in an emergency response management system to aid the deployment and support of response teams, the management of response resources, and the facilitation of inter-organizational communication and coordination.

1. Assess the existing capacity in your jurisdiction related to emergency response management systems. Identify existing systems and ascertain their relevance and suitability for public health participation, including disaster simulation, logistics management, threat tracking and management, geographic mapping for visualization of events, and emergency resource provision and management. If necessary, develop a proposal for improvements during this budget cycle.

2. Ensure participation, training, and drilling of public health personnel in the use of an emergency response management system.

3. If an adequate system does not exist with emergency response partners, implement a commercial, off-the-shelf system for the support of these functions.

4. Train and drill public health participants in the use of existing emergency response systems.

F. ENHANCED CAPACITY: to ensure full information technology support and services

1. Assess the existing capacity in your jurisdiction related to the full provision of information technology support according to industry standard practices including modern software development practices, user support practices, and ongoing monitoring and maintenance of systems. If necessary, develop a proposal for improvements during this budget cycle.

2. Implement explicit arrangements/written policies for adequate network and desktop user support, including the ability of users to obtain answers to hardware and software operational questions, repair of equipment, installation of new equipment and software, administration of servers where appropriate, and other general technical support.

3. Develop technical support staff available in an industry standard ratio of one full time equivalent support person for each 60-100 workstations covered.

4. Provide critical operational support functions with less than 24 hour alternate site provision.

5. Implement software and/or systems to support critical activities elsewhere in this guidance with appropriate redundancy, systems mirroring, and/or systems failover to provide secure and continuous access to critical IT services.

CDC Activities:

A. Provide consultation and technical assistance and training on all communication and information technology components.

B. Provide guidance on the development of the implementation of IT Functions and Specifications.

C. Facilitate the transfer of information concerning the communication and information technology activities via workshops and conferences.

D. Ensure Web-based access to information resources related to the public health aspects of detecting and responding to apparent bioterrorist incidents. In collaboration with scientists throughout CDC, develop new information and communication system resources as necessary, and implement a well-structured, Web-based presentation of CDC's preparedness and bioterrorism-related information resources to which reliable links can be made.

E. Provide updates on federal legislation and regulations that will affect communications and information technology development.

F. Serve as an ongoing referral source for technical expertise that state and local public health agencies may require in assessment, development, implementation, operation and evaluation.

G. Update communications and information technical guidance and other technical standards periodically in conjunction with industry standards and public health partners.